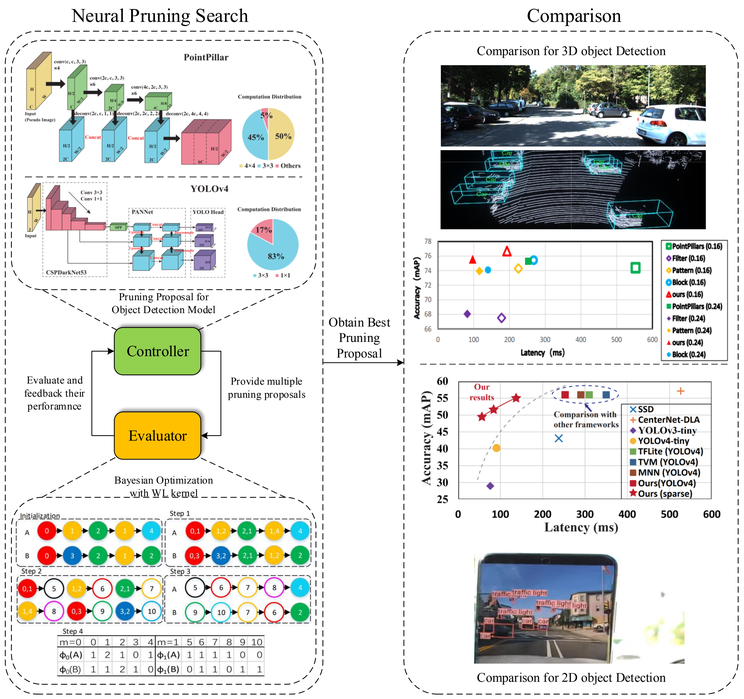
2021 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS' MEETING

SecureNN: Design of Secured Autonomous Cyber-Physical Systems Against Adversarial Machine Learning Attacks

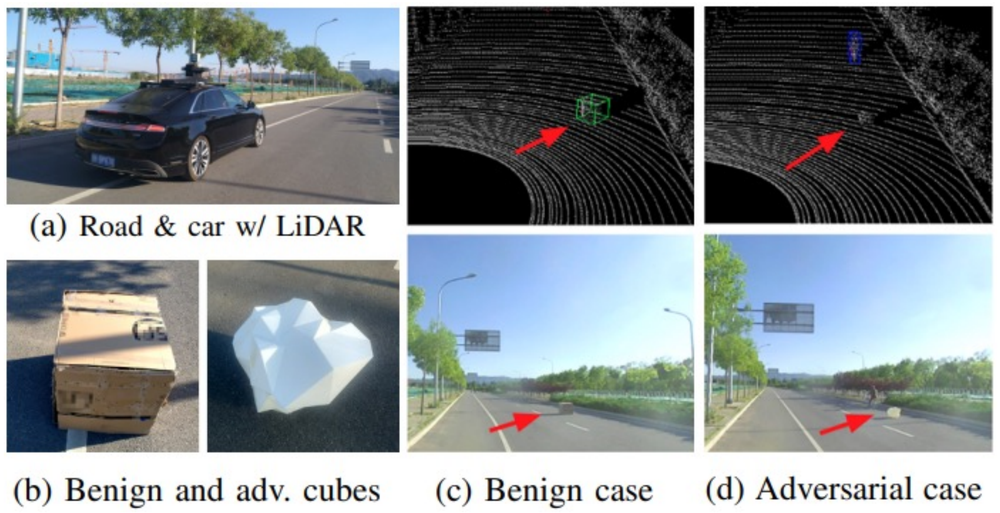
Award ID#: CNS-1932351/1932464; Nov 1, 2019 – Oct 31, 2022

Xue Lin, Northeastern University; Qi (Alfred) Chen, University of California, Irvine



Obtain Best Pruning Proposal

Towards Real-Time 2D/3D Object Detection for Autonomous Vehicles



Security of Multi-Sensor Fusion based Perception in Autonomous Driving under Physical-World Attack